Command & Control Protection
for
Force XXI Networks

AFCEA TECHNET Fort Monmouth '97
Session III

17 September 1998

BG Steven W. Boutelle

Program Executive Officer
Command, Control and Communications Systems
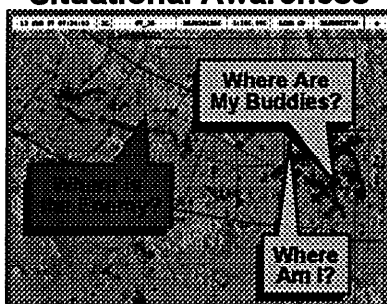
Form SF298 Citation Data

Report Date ("DD MON YYYY")01091992	Report TypeN/A	Dates Covered (from... to) ("DD MON YYYY")

Title and SubtitleCommand & Control Protection for Force XXI Networks		Contract or Grant Number
		Program Element Number
Authors		Project Number
		Task Number
		Work Unit Number
Performing Organization Name(s) and Address(es)Information Assurance Technology Analysis Center (IATAC) 3190 Fairview Park Drive Falls Church VA 22042		Performing Organization Number(s)
Sponsoring/Monitoring Agency Name(s) and Address(es)		Monitoring Agency Acronym
		Monitoring Agency Report Number(s)

Distribution/Availability StatementApproved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	

Document Classificationunclassified	Classification of SF298unclassified
Classification of Abstractunclassified	Limitation of Abstractunlimited
Number of Pages18	

REPORT DOCUMENTATION PAGE			*Form Approved* *OMB No. 074-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE 9/1/92	3. REPORT TYPE AND DATES COVERED Briefing	
4. TITLE AND SUBTITLE Command & Control Protection for Force XXI Networks			**5. FUNDING NUMBERS**
6. AUTHOR(S) Not provided			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Information Assurance Technology Analysis Center (IATAC) 3190 Fairview Park Drive Falls Church, VA 22042			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Technical Information Center DTIC-AI 8725 John J. Kingman Road, Suite 944			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES			
12a. DISTRIBUTION / AVAILABILITY STATEMENT			**12b. DISTRIBUTION CODE** A

13. ABSTRACT *(Maximum 200 Words)*

This briefing, on the Command and Control Protection for Force XXI Networks presented to AFCEA TECHNET at Fort Monmouth, NJ in 1997 by the Program Executive Officer, Command, Control and Communications Systems. It provides an overview of battlefield communications, and information system security, first digitized division. It includes host based C2 protect tools, commercial off the shelf (COTS) tools, as well as FBCB2 Security Policy.

14. SUBJECT TERMS			15. NUMBER OF PAGES
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** Unlimited

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18
298-102

Digitization Is A Key Enabler
To Gaining Information Dominance

FASTER MORE ACCURATE DECISIONS TO INFLUENCE THE BATTLEFIELD ENABLED BY INFORMATION DOMINANCE

Dominant Maneuver thru Situational Awareness

Where Are My Buddies?

Where Am I?

DISTRIBUTES SITUATIONAL AWARENESS INFORMATION RAPIDLY

Dominant Maneuver thru Collaborative Planning

PROVIDES THE CDR WITH THE ABILITY TO DISTRIBUTE ORDERS & CONVEY HIS INTENT/ORDERS QUICKLY

Precision Engagement

MOVE SENSOR & SHOOTER INFORMATION RAPIDLY
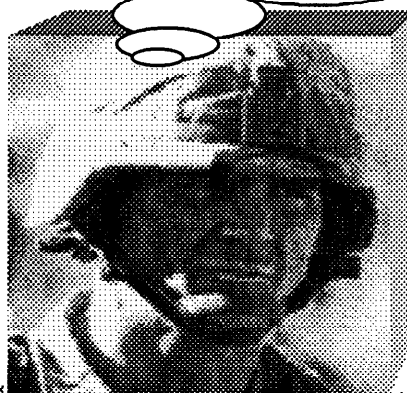
Focused Logistics
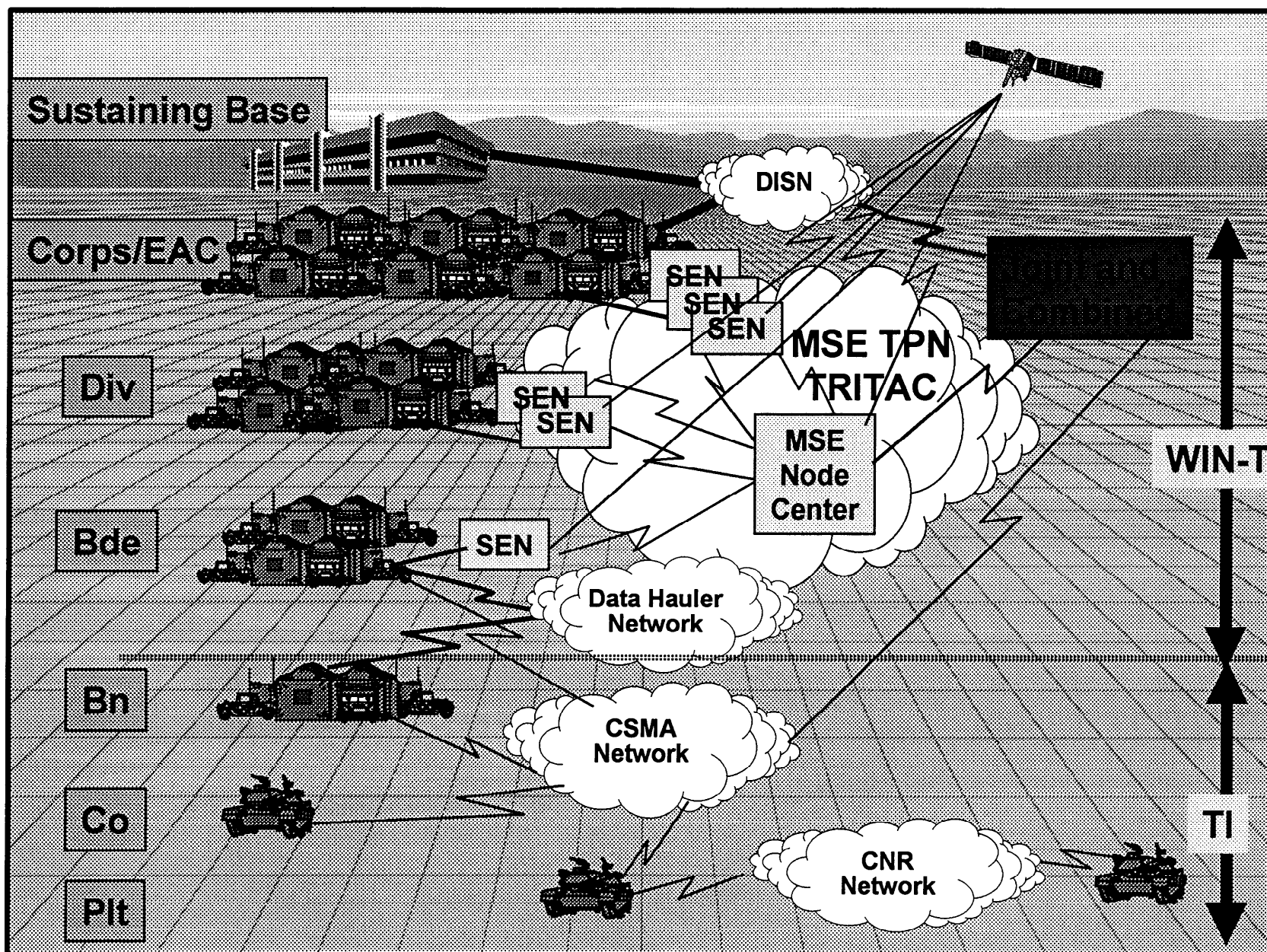

PROVIDES SUPPORT TO ANTICPATORY LOGISTICS

Dominant Maneuver thru Greater Mobility & Flexibility
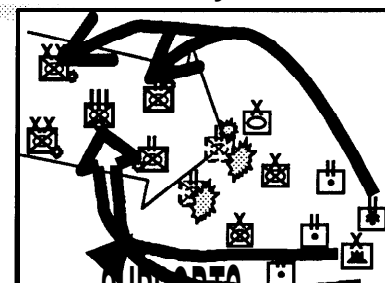
SUPPORTS THE NON-LINEAR BATTLEFIELD

Battlefield Communications Overview

Sustaining Base

Corps/EAC

Div

Bde

Bn

Co

Plt

DISN

SEN
SEN
SEN

SEN
SEN

SEN

MSE TPN
TRITAC

MSE Node Center

Data Hauler Network

CSMA Network

CNR Network

WIN-T

TI

Information System Security

Challenge

Provide commanders and their staff with information that is:

- Timely
- Accurate
- *SECURE*
- Performance and Security Balanced
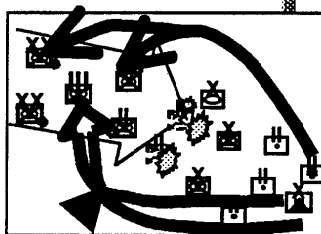
(THESE ARE ALL PROTECTION REQUIREMENTS!!!)

Command and Control Protection Tenets

- Defense in depth
- Protect, detect, & react
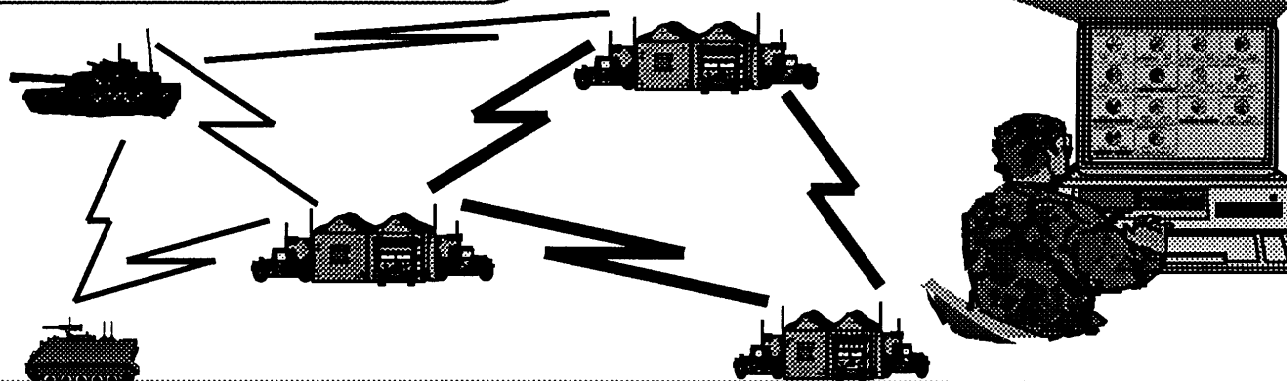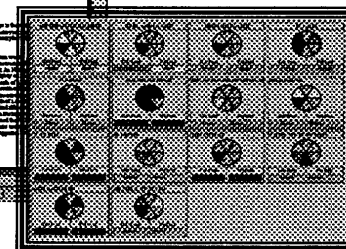
(C2P Tools, IDS, Security Mgmt)

Situation Awareness

Commander's Intent and Assessment

Directives

Intelligence. and Engagement Data

Logistic Reports

First Digitized Division (FDD) Security Architecture

1st Layer

JWICS

SIPRNET

NIPRNET

Network Intrusion Detection System

Legend

Top Secret SCI

Secret System High

Sensitive But Unclass (SBU)

Encrypted Comms

2nd Layer

Trusted Interface

SECRET SYSTEM HIGH NETWORK

Intelligence Systems

STAMIS Systems

3rd Layer

FBCB2

Network Intrusion Detection System

ABCS Systems & Office Automation

User Laptops

Back-end Connections

Legend
- ■ Firewall
- ▷ In Line Network Encryptor
- ■ Network Intrusion Device System (NIDS)
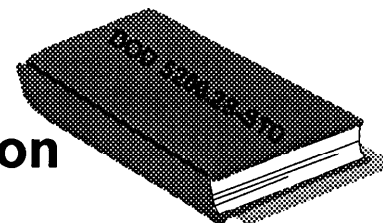
Host-Based C2 Protect

- ## Hosts Systems

  - As a minimum, all host systems will
    meet DOD 5200.28-STD Class C2 Protection
    Level Requirements

  - All hosts systems will incorporate network authentication,
    integrity, and access control mechanisms in accordance
    with the Army C2 Protect Program

  - Hosts systems will incorporate intrusion detection
    functionality to extent possible/practical

- ## Applications

  - Strong authentication, integrity, access control and
    non-repudiation mechanisms as required per service

  *Goal is to implement common
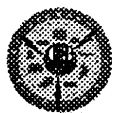 C2 Protect tools for all ABCS systems*

Host-Based C2 Protect Tools

- **TCP Wrappers to protect transaction**

- **Security Profile Inspector (SPI) to maintain configuration**

- **SWATCH to alert on audit anomalies**

  ALERT

- **Network Associates Anti-Virus**

- **Password Checkers**

Currently installed on all ABCS systems

Current "Commercial Off The Shelf" (COTS) Integration Efforts
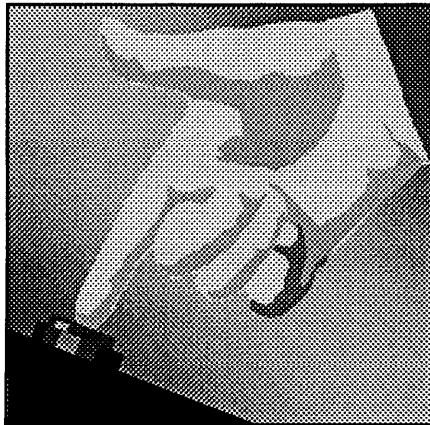
- **Purge Routines**
  - Reviewing/evaluating products available for complete memory purge to transition workstations between classified and unclassified roles

. **Secure Client - Server Services**
  - Reviewing/evaluating products that can provide
    . Authentication
    . Encryption
  - in the multiple DCE cell environment of the Tactical Operations Center

Inter-TOC and Intra-TOC Data Distribution

TOC-1

M-1068   M-1068
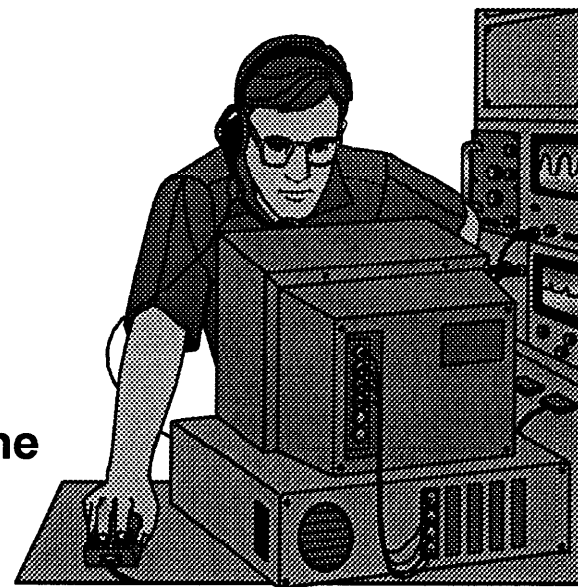
M-1068   M-1068

Mixture of clients
and servers

Inter-TOC

Current Technology
- USMTF (Sendmail-based)
- FTP and E-mail
- Web (HTTP)
- VMF
- GBS-BADD

Future Technology
- Additional VMF, GBS_BADD traffic
- Database Synchronization
- F ormalized E-Mail
- Expanded SA Service

Intra-TOC
- Database SR (Subscribing / Receiving)
- RPCs
- ORBs/MOM
- SQL Net
- WEB
- NFS, DFS

Tactical WAN

TOC 2/A-Cell

M-1068   M-1068

M-1068   M-1068

TOC 2/B-Cell

Operational Issues
- Autonomy
- Jump and Split TOCs
- Reliability
- Network Bandwidth and Contention

Inter-TOC/Inter-Cell Distribution (i.e., between servers)

Complex Architecture Must Address Many Transactions Securely

COTS Example

- Combines the strengths of Secret Key and Public Key encryption technologies

- Provides comprehensive security framework for all TCP/IP based applications

  - Includes single sign-on
    . . . in a completely transparent manner

TCP/IP

Network
(Internet, Extranet,
Intranet)

Application Server

Desktop Client --
TCP/IP Applications

Security Server
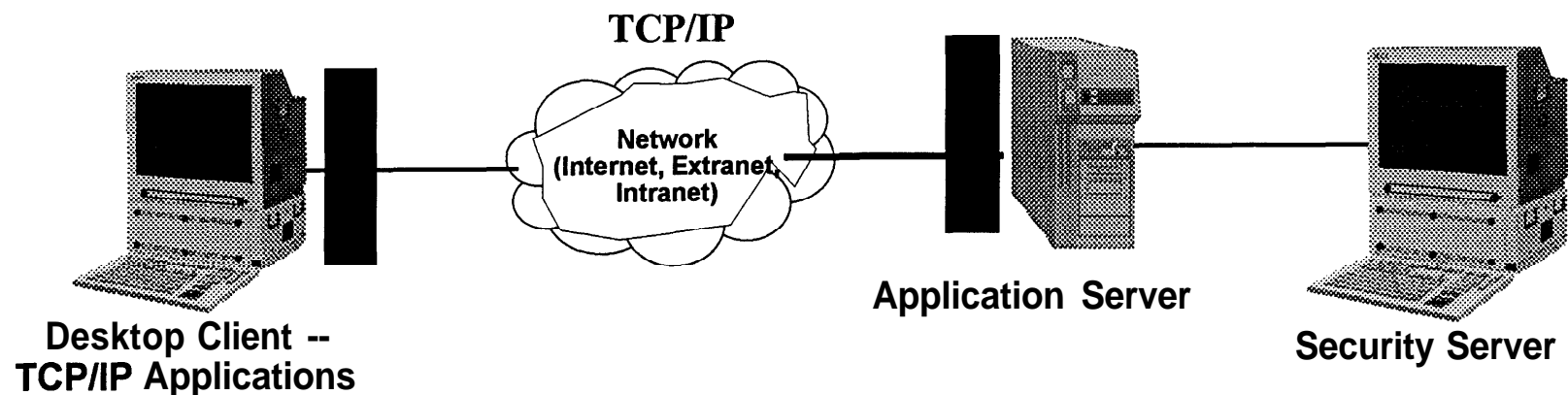
COTS Secure Capabilities

- **Authentication and single sign-on**

- **Standardized authorization across all applications**

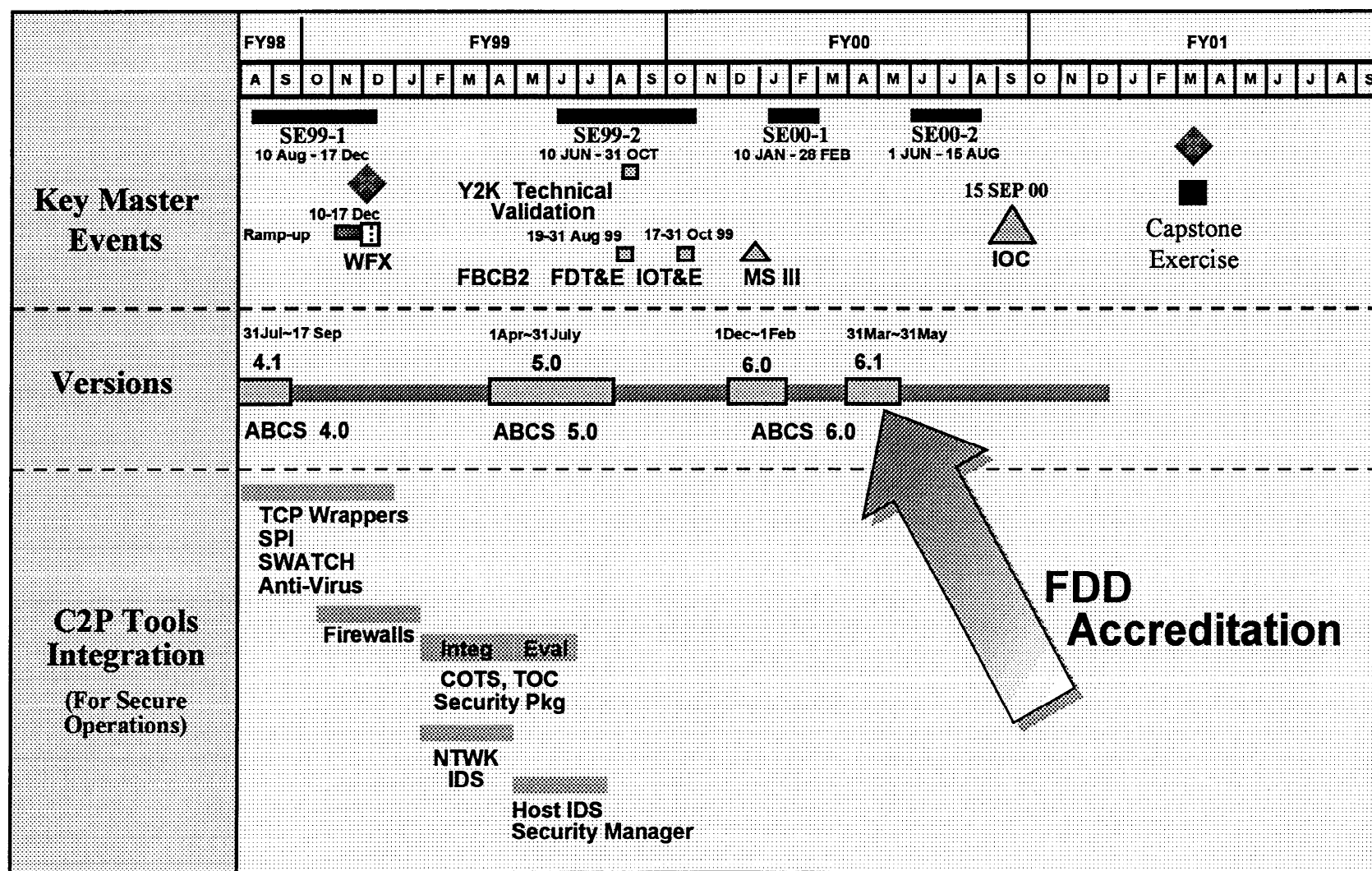- **Data protection services, smart Virtual Private Network (VPN)**

Centralized Management
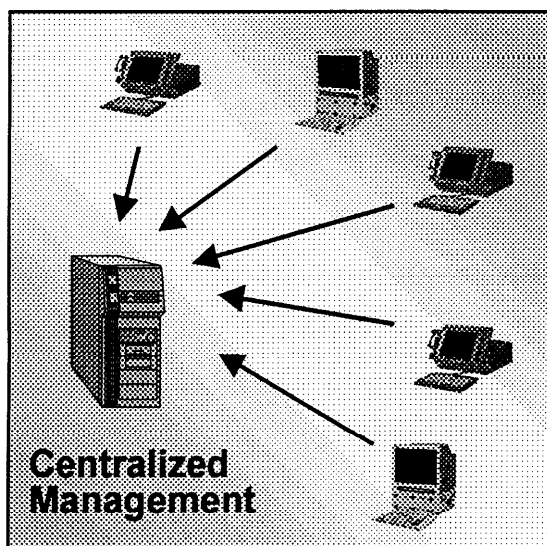
- **Dynamic support for new protocols**

- **Centralized management, connection monitoring**

- **Auditing, accounting, event notification**

- **Public key certificate services**

C2 Protect Integration
Master FDD Schedule (Version 1.3)

FY98	FY99	FY00	FY01
A S	O N D J F M A M J J A	S O N D J F M A M J J A	S O N D J F M A M J J A S

Key Master Events

SE99-1
10 Aug - 17 Dec

SE99-2
10 JUN - 31 OCT

SE00-1
10 JAN - 28 FEB

SE00-2
1 JUN - 15 AUG

10-17 Dec

Y2K Technical Validation

15 SEP 00

Ramp-up

19-31 Aug 99   17-31 Oct 99

WFX

FBCB2   FDT&E   IOT&E   MS III

IOC

Capstone Exercise

Versions

31Jul~17 Sep
4.1

1Apr~31July
5.0

1Dec~1Feb
6.0

31Mar~31May
6.1

ABCS 4.0   ABCS 5.0   ABCS 6.0

C2P Tools Integration
(For Secure Operations)

TCP Wrappers
SPI
SWATCH
Anti-Virus

Firewalls

Integ   Eval

COTS, TOC
Security Pkg

NTWK
IDS

Host IDS
Security Manager

FDD Accreditation

FBCB2 Initial Protection Capabilities
Oct '99

- **FBCB2 authenticates to the router upon request to grant/validate network access**

- **Access control to data based on clearance level**

  - **Clears C2 data when operational level lower ed to SBU**

- **Capability for any user to initiate both disk overwrite and resetting of the router to factory default**

- **Audit reports generated and forwarded to designated collection points**
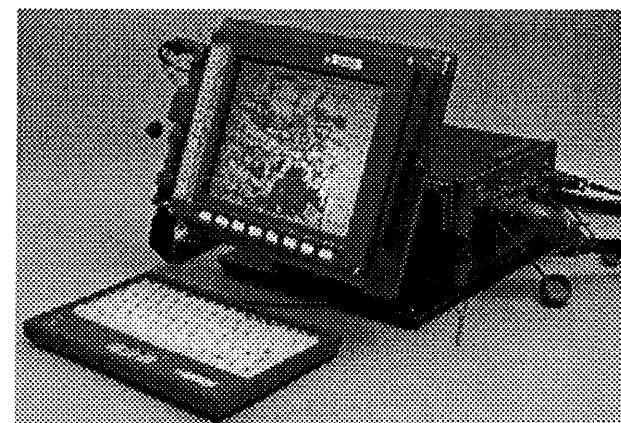
FBCB2: Force XXI Battle Command Brigade and Below

FBCB2 Capabilities Planned for FDD
Sep '00

- **Remote security management**
  - Load passwords
  - Control system access: three operational capabilities
    - Challenge a user to re-authenticate without interfering with the mission
    - Lock-out the user until re-authentication
    - Disable - through overwrite of the disk and reset of the router to its factory default
  - Authentication through the use of digital signature
    - Security management transactions initiated/signed by security manager and sent to remote FBCB2

- **Ongoing evaluation of C2 Protection enhancements**
  - Message authentication, intrusion detection, malicious code detection

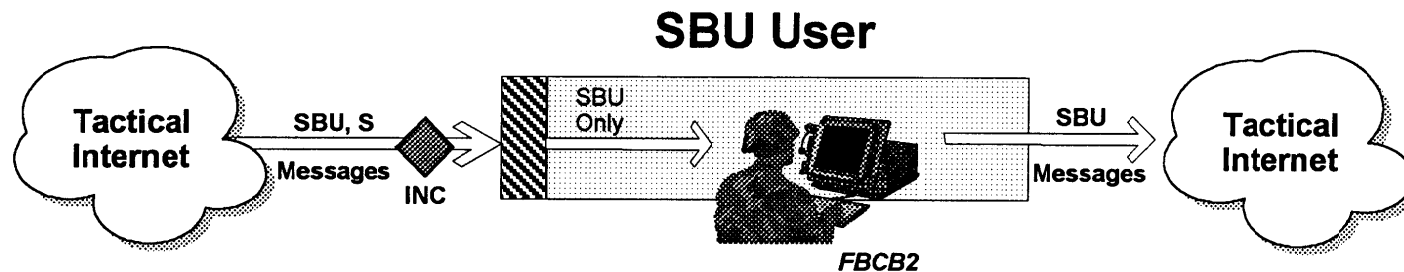**FBCB2:** Force XXI Battle Command Brigade and Below

Summary FBCB2 Security Policy

Each Computer Maintains a SECRET System High Posture
Discretionary Access Control (DAC) of SECRET Data is Enforced at End-Points

At Sending End -
Manual review required
for message remark

At Receiving End -
Hard rejection of messages
marked above User level

Secret User

Tactical Internet — SBU, S Messages — INC — SBU, S — FBCB2 — Human Review and "Remark" — S / SBU Messages — Tactical Internet

SBU User

Tactical Internet — SBU, S Messages — INC — SBU Only — FBCB2 — SBU Messages — Tactical Internet

---

Legend

| | Message Rejection | | Message Remarked | SBU Sensitive But Unclassified | S Secret |

Future Force XXI C2P

- **Selective Purge**

- **Host Intrusion Detection Systems**

- **Tactical network guards to allow information exchange automatically between classification levels**

Warfighter Information Network - Terrestrial (WIN-T)

Sensitive But Unclassified User

Network Guard

Network Guard

Secret User
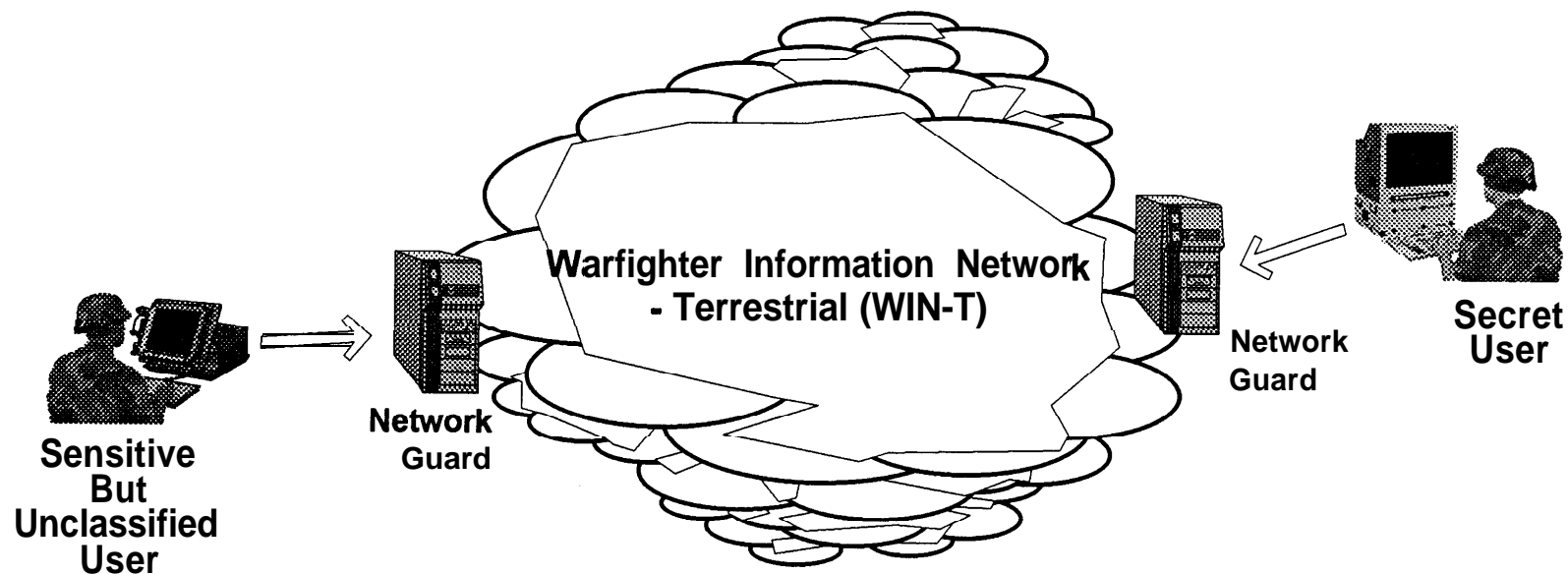
Summary

- Information Assurance (IA) is a proactive and imperative part of the Army Digitization Program

- PEO C3S PMs will continue to aggressively pursue emerging assurance technologies, e.g.

  -Smart cards for user authentication

Biometrics for Access Control

- Biometrics for access control

- Personal / host-level firewalls

- . . . .